Disappearing Cryptography Third Edition Information Hiding Steganography Watermarking The Morgan Kaufmann Series In Software Engineering And Programming

When somebody should go to the ebook stores, search inauguration by shop, shelf by shelf, it is in reality problematic. This is why we give the ebook compilations in this website. It will agreed ease you to see guide **disappearing cryptography third edition information hiding steganography watermarking the morgan kaufmann series in software engineering and programming** as you such as.

By searching the title, publisher, or authors of guide you truly want, you can discover them rapidly. In the house, workplace, or perhaps in your method can be every best area within net connections. If you target to download and install the disappearing cryptography third edition information hiding steganography watermarking the morgan kaufmann series in software engineering and programming, it is no question easy then, in the past currently we extend the join to purchase and make bargains to download and install disappearing cryptography third edition information hiding steganography watermarking the morgan kaufmann series in software engineering and programming for that reason simple!

The Dialogical Roots of Deduction - Catarina Dutilh Novaes 2020-12-17
The first comprehensive account of the concept and practices of deduction covering philosophy, history, cognition and mathematical practice.
CompTIA Security+ Study Guide - Emmett Dulaney 2017-10-05
Some copies of CompTIA Security+ Study Guide: Exam SY0-501 (9781119416876) were printed without discount exam vouchers in the front of the books. If you did not receive a discount exam voucher with your book, please visit http://media.wiley.com/product_ancillary/5X/11194168/DOWNLOAD/CompTIA_Coupon.pdf to download one. Expert preparation covering 100% of Security+ exam SY0-501 objectives CompTIA Security+ Study Guide, Seventh Edition offers invaluable preparation for Exam SY0-501. Written by an expert author team, this book covers 100% of the exam objectives with clear, concise explanation. You'll learn how to handle threats, attacks, and vulnerabilities using industry-standard tools and technologies, while understanding the role of architecture and design. From everyday tasks like identity and access management to complex topics like risk management and cryptography, this study guide helps you consolidate your knowledge base in preparation for the Security+ exam. Practical examples illustrate how these processes play out in real-world scenarios, allowing you to immediately translate essential concepts to on-the-job application. You also gain access to the Sybex online learning environment, which features a robust toolkit for more thorough prep: flashcards, glossary of key terms, practice questions, and a pre-assessment exam equip you with everything you need to enter the exam confident in your skill set. This study guide is approved and endorsed by CompTIA, and has been fully updated to align with the latest version of the exam. Master essential security technologies, tools, and tasks Understand how Security+ concepts are applied in the real world Study on the go with electronic flashcards and more Test your knowledge along the way with hundreds of practice questions To an employer, the CompTIA Security+ certification proves that you have the knowledge base and skill set to secure applications, devices, and networks;

analyze and respond to threats; participate in risk mitigation, and so much more. As data threats loom larger every day, the demand for qualified security professionals will only continue to grow. If you're ready to take the first step toward a rewarding career, CompTIA Security+ Study Guide, Seventh Edition is the ideal companion for thorough exam preparation.

Disappearing Cryptography - Peter Wayner 2009-06-12

Cryptology is the practice of hiding digital information by means of various obfuscatory and steganographic techniques. The application of said techniques facilitates message confidentiality and sender/receiver identity authentication, and helps to ensure the integrity and security of computer passwords, ATM card information, digital signatures, DVD and HDDVD content, and electronic commerce. Cryptography is also central to digital rights management (DRM), a group of techniques for technologically controlling the use of copyrighted material that is being widely implemented and deployed at the behest of corporations that own and create revenue from the hundreds of thousands of mini-transactions that take place daily on programs like iTunes. This new edition of our best-selling book on cryptography and information hiding delineates a number of different methods to hide information in all types of digital media files. These methods include encryption, compression, data embedding and watermarking, data mimicry, and scrambling. During the last 5 years, the continued advancement and exponential increase of computer processing power have enhanced the efficacy and scope of electronic espionage and content appropriation. Therefore, this edition has amended and expanded outdated sections in accordance with new dangers, and includes 5 completely new chapters that introduce newer more sophisticated and refined cryptographic algorithms and techniques (such as fingerprinting, synchronization, and quantization) capable of withstanding the evolved forms of attack. Each chapter is divided into sections, first providing an introduction and high-level summary for those who wish to understand the concepts without wading through technical explanations, and then presenting concrete examples and greater detail for those who want to write their own programs. This combination of practicality and theory allows programmers and system designers to not only implement tried and true encryption procedures, but also consider probable future developments in their designs, thus fulfilling the need for preemptive caution that is becoming ever more explicit as the transference of digital media escalates. Includes 5 completely new chapters that delineate the most current and sophisticated cryptographic algorithms, allowing readers to protect their information against even the most evolved electronic attacks Conceptual tutelage in conjunction with detailed mathematical directives allows the reader to not only understand encryption procedures, but also to write programs which anticipate future security developments in their design

Library Journal - 2002

Leading Issues in Information Warfare and Security Research - Julie Ryan 2011

As virtually every aspect of society becomes increasingly dependent on information and communications technology, so our vulnerability to attacks on this technology increases. This is a major theme of this collection of leading edge research papers. At the same time there is another side to this issue, which is if the technology can be used against society by the purveyors of malware etc., then technology may also be used positively in the pursuit of society's objectives. Specific topics in the collection include Cryptography and Steganography, Cyber Antagonism, Information Sharing Between Government and Industry as a Weapon, Terrorist Use of the Internet, War and Ethics in Cyberspace to name just a few. The papers in this book take a wide ranging look at the more important issues surrounding the use of information and communication technology as it applies to the security of vital systems that can have a major impact on the functionality of our society. This book includes leading contributions to research in this field from 9 different countries and an introduction to the subject by Professor Julie Ryan from George Washington University in the USA.

Beginning Cryptography with Java - David Hook 2005-11-02

Beginning Cryptography with Java While

cryptography can still be a controversial topic in theprogramming community, Java has weathered that storm and provides arich set of APIs that allow you, the developer, to effectivelyinclude cryptography in applications-if you know how. This book teaches you how. Chapters one through five cover thearchitecture of the JCE and JCA, symmetric and asymmetric keyencryption in Java, message authentication codes, and how to createJava implementations with the API provided by the Bouncy CastleASN.1 packages, all with plenty of examples. Building on thatfoundation, the second half of the book takes you into higher-leveltopics, enabling you to create and implement secure Javaapplications and make use of standard protocols such as CMS, SSL,and S/MIME. What you will learn from this book How to understand and use JCE, JCA, and the JSSE for encryptionand authentication The ways in which padding mechanisms work in ciphers and how tospot and fix typical errors An understanding of how authentication mechanisms areimplemented in Java and why they are used Methods for describing cryptographic objects with ASN.1 How to create certificate revocation lists and use the OnlineCertificate Status Protocol (OCSP) Real-world Web solutions using Bouncy Castle APIs Who this book is for This book is for Java developers who want to use cryptography intheir applications or to understand how cryptography is being usedin Java applications. Knowledge of the Java language is necessary,but you need not be familiar with any of the APIs discussed. Wrox Beginning guides are crafted to make learningprogramming languages and technologies easier than you think,providing a structured, tutorial format that will guide you throughall the techniques involved.

Information Hiding - Jan Camenisch 2007-09-18

These proceedings contain the 25 papers that were accepted for presentation at the Eighth Information Hiding Conference, held July 10-12, 2006 in Old Town Alexandria, Virginia. The paperswere selectedby the ProgramCommittee from more than 70 submissions on the basis of their novelty, originality, and scienti?c merit. We aregratefulto allauthorswho submitted their workforconsideration. The papers were divided into ten sessions [Watermarking, Information Hiding and Networking, Data Hiding in Unusual Content (2 sessions), Fundamentals, Software Protection, Steganalysis, Steganography (2 sessions), and Subliminal Channels], showing the breadth of research in the?eld. This year was an imp- tant one in the history of the IHW: "Workshop" was dropped from the name to show that the?eld has matured andthat the conference has become the premier venue for the dissemination of new results. The conference employed a double-blind reviewing process. Each paper was examined by at least three reviewers. Papers submitted by ProgramCommittee members were held to a higher standard. We relied on the advice of outside colleagues and would like to extend our thanks for their contribution to the paper selection process and their dedication to excellence in research.

Information Security Policies and Actions in Modern Integrated Systems - Mariagrazia Fugini 2004-01-01

This work discusses research in theoretical and practical aspects of security in distributed systems, in particular in information systems and related security tools. Topics include XML-based management systems, security of multimedia data, and technology and use of smart cards.

Blown to Bits - Harold Abelson 2008

'Blown to Bits' is about how the digital explosion is changing everything. The text explains the technology, why it creates so many surprises and why things often don't work the way we expect them to. It is also about things the information explosion is destroying: old assumptions about who is really in control of our lives.

Data Hiding - Michael T. Raggo 2012-12-31

As data hiding detection and forensic techniques have matured, people are creating more advanced stealth methods for spying, corporate espionage, terrorism, and cyber warfare all to avoid detection. Data Hiding provides an exploration into the present day and next generation of tools and techniques used in covert communications, advanced malware methods and data concealment tactics. The hiding techniques outlined include the latest technologies including mobile devices,

multimedia, virtualization and others. These concepts provide corporate, goverment and military personnel with the knowledge to investigate and defend against insider threats, spy techniques, espionage, advanced malware and secret communications. By understanding the plethora of threats, you will gain an understanding of the methods to defend oneself from these threats through detection, investigation, mitigation and prevention. Provides many real-world examples of data concealment on the latest technologies including iOS, Android, VMware, MacOS X, Linux and Windows 7 Dives deep into the less known approaches to data hiding, covert communications, and advanced malware Includes never before published information about next generation methods of data hiding Outlines a well-defined methodology for countering threats Looks ahead at future predictions for data hiding

Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses - M.N. Ogun 2015-10-08

ICT plays a crucial role in the pursuit of modernization in the countries of Slovenia, Croatia, Albania and Bulgaria, which form the South Eastern European (SEE) region., The quest for Euro-Atlantic integration and the undeniable necessity for direct foreign investment have encouraged the SEE countries to invest in the development of cyber technology, and it has become the dominant area for social, economic and political interaction within the region. This has had both positive and negative consequences. This book presents the proceedings of the NATO Advanced Training Course (ATC), held in Ohrid, former Yugoslav Republic of Macedonia, in December 2014. The ATC addressed serious concerns about terrorist use of cyber technology in South Eastern Europe, which not only has the potential to destabilize regional efforts to create a platform for increased development by creating a breeding ground for the training of extremists and the launching of cyber attacks, but also represents a direct and indirect threat to the security and stability of other NATO partner countries. The book will be of interest to all those involved in countering the threat posed by terrorist use of the Internet worldwide.

Security and Privacy in Digital Economy - Shui Yu 2020-10-22

This book constitutes the refereed proceedings of the First International Conference on Security and Privacy in Digital Economy, SPDE 2020, held in Quzhou, China, in October 2020*. The 49 revised full papers and 2 short papers were carefully reviewed and selected from 132 submissions. The papers are organized in topical sections: cyberspace security, privacy protection, anomaly and intrusion detection, trust computation and forensics, attacks and countermeasures, covert communication, security protocol, anonymous communication, security and privacy from social science. *The conference was held virtually due to the COVID-19 pandemic.

Digital Privacy and Security Using Windows - Nihad Hassan 2017-07-02

Use this hands-on guide to understand the ever growing and complex world of digital security. Learn how to protect yourself from digital crime, secure your communications, and become anonymous online using sophisticated yet practical tools and techniques. This book teaches you how to secure your online identity and personal devices, encrypt your digital data and online communications, protect cloud data and Internet of Things (IoT), mitigate social engineering attacks, keep your purchases secret, and conceal your digital footprint. You will understand best practices to harden your operating system and delete digital traces using the most widely used operating system, Windows. Digital Privacy and Security Using Windows offers a comprehensive list of practical digital privacy tutorials in addition to being a complete repository of free online resources and tools assembled in one place. The book helps you build a robust defense from electronic crime and corporate surveillance. It covers general principles of digital privacy and how to configure and use various security applications to maintain your privacy, such as TOR, VPN, and BitLocker. You will learn to encrypt email communications using Gpg4win and Thunderbird. What You'll Learn Know the various parties interested in having your private data Differentiate between government and corporate surveillance, and the motivations behind each one Understand how online tracking works technically Protect digital

data, secure online communications, and become anonymous online Cover and destroy your digital traces using Windows OS Secure your data in transit and at rest Be aware of cyber security risks and countermeasures Who This Book Is For End users, information security professionals, management, infosec students

ECIW2010- Proceedings of the 9th European Conference on Information Warfare and Security - Josef Demergis 2010-01-07

Windows Registry Forensics - Harlan Carvey 2011-01-03

Windows Registry Forensics provides the background of the Windows Registry to help develop an understanding of the binary structure of Registry hive files. Approaches to live response and analysis are included, and tools and techniques for postmortem analysis are discussed at length. Tools and techniques are presented that take the student and analyst beyond the current use of viewers and into real analysis of data contained in the Registry, demonstrating the forensic value of the Registry. Named a 2011 Best Digital Forensics Book by InfoSec Reviews, this book is packed with real-world examples using freely available open source tools. It also includes case studies and a CD containing code and author-created tools discussed in the book. This book will appeal to computer forensic and incident response professionals, including federal government and commercial/private sector contractors, consultants, etc. Named a 2011 Best Digital Forensics Book by InfoSec Reviews Packed with real-world examples using freely available open source tools Deep explanation and understanding of the Windows Registry – the most difficult part of Windows to analyze forensically Includes a CD containing code and author-created tools discussed in the book

Forthcoming Books - Rose Arny 2002-04

Security in Computing - Charles P. Pfleeger 2009

Techno-Societal 2020 - Prashant M. Pawar 2021-05-19

This book, divided in two volumes, originates from Techno-Societal 2020: the 3rd International Conference on Advanced Technologies for Societal Applications, Maharashtra, India, that brings together faculty members of various engineering colleges to solve Indian regional relevant problems under the guidance of eminent researchers from various reputed organizations. The focus of this volume is on technologies that help develop and improve society, in particular on issues such as sensor and ICT based technologies for the betterment of people, Technologies for agriculture and healthcare, micro and nano technological applications. This conference aims to help innovators to share their best practices or products developed to solve specific local problems which in turn may help the other researchers to take inspiration to solve problems in their region. On the other hand, technologies proposed by expert researchers may find applications in different regions. This offers a multidisciplinary platform for researchers from a broad range of disciplines of Science, Engineering and Technology for reporting innovations at different levels.

Computer and Information Security Handbook - John R. Vacca 2009-05-04

Presents information on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats. Also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to implement security policies and procedures. In addition, this book covers security and network design with respect to particular vulnerabilities and threats. It also covers risk assessment and mitigation and auditing and testing of security systems as well as application standards and technologies required to build secure VPNs, configure client software and server operating systems, IPsec-enabled routers, firewalls and SSL clients. This comprehensive book will provide essential knowledge and skills needed to select, design and deploy a public key infrastructure (PKI) to secure existing and future applications. * Chapters contributed by leaders in the field cover theory and practice of computer security technology, allowing the reader to develop a new level of technical

expertise * Comprehensive and up-to-date coverage of security issues facilitates learning and allows the reader to remain current and fully informed from multiple viewpoints * Presents methods of analysis and problem-solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

Steganography in Digital Media - Jessica Fridrich 2010

Understand the building blocks of covert communication in digital media and apply the techniques in practice with this self-contained guide.

Information Hiding - Mauro Barni 2005-11-24

This book constitutes the thoroughly refereed post-proceedings of the7th International Workshop on Information Hiding, IH 2005, held in Barcelona, Spain in June 2005. The 28 revised full papers presented together with an invited talk werecarefully selected from 90 papers submitted. The papers are organized in topical sections on anonymity, watermarking, theory, watermark attacks, steganography, hiding in unusual content, steganalysis, software watermarking, and fingerprinting.

Digital Watermarking - Anthony T. S. Ho 2009-08-17

This book constitutes the refereed proceedings of the 8th Interntaional Workshop, IWDW 2009, held in Guildford, Surrey, UK, August 24-26, 2009. The 25 revised full papers, including 4 poster presentations, presented together with 3 invited papers were carefully reviewed and selected from 50 submissions. The papers are organized in topical sections on robust watermarking, video watermarking, steganography and steganalysis, multimedia watermarking and security protocols, as well as image forensics and authentication.

ICICS 2004 - Javier Lopez 2004-10-15

This book constitutes the refereed proceedings of the 6th International Conference on Information and Communications Security, ICICS 2004, held in Malaga, Spain in October 2004. The 42 revised full papers presented were carefully reviewed and selected from 245 submissions. The papers address a broad range of topics in information and communication security including digital signatures, group signature schemes, e-commerce, digital payment systems, cryptographic attacks, mobile networking, authentication, channel analysis, power-analysis attacks, mobile agent security, broadcast encryption, AES, security analysis, XTR, access control, and intrusion detection.

Wi-Foo - Andrew A. Vladimirov 2004

The definitive guide to penetrating and defending wireless networks. Straight from the field, this is the definitive guide to hacking wireless networks. Authored by world-renowned wireless security auditors, this hands-on, practical guide covers everything you need to attack -- or protect -- any wireless network. The authors introduce the 'battlefield, ' exposing today's 'wide open' 802.11 wireless networks and their attackers. One step at a time, you'll master the attacker's entire arsenal of hardware and software tools: crucial knowledge for crackers and auditors alike. Next, you'll learn systematic countermeasures for building hardened wireless 'citadels''including cryptography-based techniques, authentication, wireless VPNs, intrusion detection, and more. Coverage includes: Step-by-step walkthroughs and explanations of typical attacks Building wireless hacking/auditing toolkit: detailed recommendations, ranging from discovery tools to chipsets and antennas Wardriving: network mapping and site surveying Potential weaknesses in current and emerging standards, including 802.11i, PPTP, and IPSec Implementing strong, multilayered defenses Wireless IDS: why attackers aren't as untraceable as they think Wireless hacking and the law: what's legal, what isn't If you're a hacker or security auditor, this book will get you in. If you're a netadmin, sysadmin, consultant, or home user, it will keep everyone else out.

Cryptography 101: From Theory to Practice - Rolf Oppliger 2021-06-30

This exciting new resource provides a comprehensive overview of the field of cryptography and the current state of the art. It delivers an overview about cryptography as a field of study and the various unkeyed, secret key, and public key cryptosystems that are available, and it then delves more deeply into the technical details of the systems. It introduces, discusses, and puts into perspective the cryptographic technologies and techniques, mechanisms, and systems that are available

today. Random generators and random functions are discussed, as well as one-way functions and cryptography hash functions. Pseudorandom generators and their functions are presented and described. Symmetric encryption is explored, and message authentical and authenticated encryption are introduced. Readers are given overview of discrete mathematics, probability theory and complexity theory. Key establishment is explained. Asymmetric encryption and digital signatures are also identified. Written by an expert in the field, this book provides ideas and concepts that are beneficial to novice as well as experienced practitioners.

Emergent Strategies for E-Business Processes, Services and Implications: Advancing Corporate Frameworks - Lee, In 2008-12-31

"This book presents a collection of research associated with the emerging e-business technologies and applications, attempting to stimulate the advancement of various e-business frameworks and applications, and to provide future research directions"--Provided by publisher.

Steganography and Watermarking - Ching-Nung Yang 2013-01-01

Privacy and Copyright protection is a very important issue in our digital society, where a very large amount of multimedia data are generated and distributed daily using different kinds of consumer electronic devices and very popular communication channels, such as the Web and social networks. This book "Steganography and Watermarking" introduces state-of-the-art technology on data hiding and copyright protection of digital images, and offers a solid basis for future study and research. Steganographic technique overcomes the traditional cryptographic approach, providing new solutions for secure data transmission without raising users' malicious intention. In steganography, some secret information can be inserted into the original data in imperceptible and efficient ways to avoid distortion of the image, and enhance the embedding capacity, respectively. Digital watermarking also adopts data hiding techniques for copyright protection and tampering verification of multimedia data. In watermarking, an illegitimate copy can be recognized by testing the presence of a valid watermark and a dispute on the ownership of the image resolved. Different kinds of steganographic and watermarking techniques, providing different features and diverse characteristics, have been presented in this book. This book provides a reference for theoretical problems as well as practical solutions and applications for steganography and watermarking techniques. In particular, both the academic community (graduate student, post-doc and faculty) in Electrical Engineering, Computer Science, and Applied Mathematics; and the industrial community (engineers, engineering managers, programmers, research lab staff and managers, security managers) will find this book interesting.

Everyday Cryptography - Keith Martin 2017-06-22

Cryptography is a vital technology that underpins the security of information in computer networks. This book presents a comprehensive introduction to the role that cryptography plays in providing information security for everyday technologies such as the Internet, mobile phones, Wi-Fi networks, payment cards, Tor, and Bitcoin. This book is intended to be introductory, self-contained, and widely accessible. It is suitable as a first read on cryptography. Almost no prior knowledge of mathematics is required since the book deliberately avoids the details of the mathematics techniques underpinning cryptographic mechanisms. Instead our focus will be on what a normal user or practitioner of information security needs to know about cryptography in order to understand the design and use of everyday cryptographic applications. By focusing on the fundamental principles of modern cryptography rather than the technical details of current cryptographic technology, the main part this book is relatively timeless, and illustrates the application of these principles by considering a number of contemporary applications of cryptography. Following the revelations of former NSA contractor Edward Snowden, the book considers the wider societal impact of use of cryptography and strategies for addressing this. A reader of this book will not only be able to understand the everyday use of cryptography, but also be able to interpret

future developments in this fascinating and crucially important area of technology.

Applied Cryptography - Bruce Schneier 2015

From the world's most renowned security technologist, Bruce Schneier, this 20th Anniversary Edition is the most definitive reference on cryptography ever published and is the seminal work on cryptography. Cryptographic techniques have applications far beyond the obvious uses of encoding and decoding information. For developers who need to know about capabilities, such as digital signatures, that depend on cryptographic techniques, there's no better overview than Applied Cryptography, the definitive book on the subject. Bruce Schneier covers general classes of cryptographic protocols and then specific techniques, detailing the inner workings of real-world cryptographic algorithms including the Data Encryption Standard and RSA public-key cryptosystems. The book includes source-code listings and extensive advice on the practical aspects of cryptography implementation, such as the importance of generating truly random numbers and of keeping keys secure. ". . .the best introduction to cryptography I've ever seen. . . .The book the National Security Agency wanted never to be published. . . ." -Wired Magazine ". . .monumental . . . fascinating . . . comprehensive . . . the definitive work on cryptography for computer programmers . . ." -Dr. Dobb's Journal ". . .easily ranks as one of the most authoritative in its field." -PC Magazine The book details how programmers and electronic communications professionals can use cryptography-the technique of enciphering and deciphering messages-to maintain the privacy of computer data. It describes dozens of cryptography algorithms, gives practical advice on how to implement them into cryptographic software, and shows how they can be used to solve security problems. The book shows programmers who design computer applications, networks, and storage systems how they can build security into their software and systems. With a new Introduction by the author, this premium edition will be a keepsake for all those committed to computer and cyber security.

Optical and Digital Techniques for Information Security - Bahram Javidi 2006-11-22

There are wide-ranging implications in information security beyond national defense. Securing our information has implications for virtually all aspects of our lives, including protecting the privacy of our ?nancial transactions and medical records, facilitating all operations of government, maintaining the integrity of national borders, securing important facilities, ensuring the safety of our food and commercial products, protecting the safety of our aviation system—even safeguarding the integrity of our very identity against theft. Information security is a vital element in all of these activities, particularly as information collection and distribution become ever more connected through electronic information delivery systems and commerce. This book encompasses results of research investigation and technologies that can be used to secure, protect, verify, and authenticate objects and inf- mation from theft, counterfeiting, and manipulation by unauthorized persons and agencies. The book has drawn on the diverse expertise in optical sciences and engineering, digital image processing, imaging systems, information p- cessing, mathematical algorithms, quantum optics, computer-based infor- tion systems, sensors, detectors, and biometrics to report novel technologies that can be applied to information-security issues. The book is unique because it has diverse contributions from the ?eld of optics, which is a new emerging technology for security, and digital techniques that are very accessible and can be interfaced with optics to produce highly e?ective security systems.

Information Hiding - 2005

Secure and Resilient Software Development - Mark S. Merkow 2010-06-16

Although many software books highlight open problems in secure software development, few provide easily actionable, ground-level solutions. Breaking the mold, Secure and Resilient Software Development teaches you how to apply best practices and standards for consistent and secure software development. It details specific quality software developmen

Cryptography Apocalypse Roger A. Grimes 2019-11-12

Will your organization be protected the day a quantum computer breaks encryption on the

internet? Computer encryption is vital for protecting users, data, and infrastructure in the digital age. Using traditional computing, even common desktop encryption could take decades for specialized ‘crackers’ to break and government and infrastructure-grade encryption would take billions of times longer. In light of these facts, it may seem that today’s computer cryptography is a rock-solid way to safeguard everything from online passwords to the backbone of the entire internet. Unfortunately, many current cryptographic methods will soon be obsolete. In 2016, the National Institute of Standards and Technology (NIST) predicted that quantum computers will soon be able to break the most popular forms of public key cryptography. The encryption technologies we rely on every day—HTTPS, TLS, WiFi protection, VPNs, cryptocurrencies, PKI, digital certificates, smartcards, and most two-factor authentication—will be virtually useless. . . unless you prepare. Cryptography Apocalypse is a crucial resource for every IT and InfoSec professional for preparing for the coming quantum-computing revolution. Post-quantum crypto algorithms are already a reality, but implementation will take significant time and computing power. This practical guide helps IT leaders and implementers make the appropriate decisions today to meet the challenges of tomorrow. This important book: Gives a simple quantum mechanics primer Explains how quantum computing will break current cryptography Offers practical advice for preparing for a post-quantum world Presents the latest information on new cryptographic methods Describes the appropriate steps leaders must take to implement existing solutions to guard against quantum-computer security threats Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto is a must-have guide for anyone in the InfoSec world who needs to know if their security is ready for the day crypto break and how to fix it.

Security and Privacy in Communication Networks - Sushil Jajodia 2010-11-29

This book constitutes the thoroughly refereed proceedings of the 6th International ICST Conference, SecureComm 2010, held in Singapore in September 2010. The 28 revised full papers were carefully reviewed and selected from 112 submissions. They are organized in topical sections on malware and email security, anonymity and privacy, wireless security, systems security, network security, and security protocols.

Disappearing Cryptography - Peter Wayner 2009

This new edition of cryptography and information hiding delineates a number of different methods to hide information in all types of digitalmedia files. These methods include encryption, compression, data embedding and watermarking,data mimicry, and scrambling.

Multimedia Forensics and Security - Li, Chang-Tsun 2008-07-31

As information technology is rapidly progressing, an enormous amount of media can be easily exchanged through Internet and other communication networks. Increasing amounts of digital image, video, and music have created numerous information security issues and is now taken as one of the top research and development agendas for researchers, organizations, and governments worldwide. Multimedia Forensics and Security provides an in-depth treatment of advancements in the emerging field of multimedia forensics and security by tackling challenging issues such as digital watermarking for copyright protection, digital fingerprinting for transaction tracking, and digital camera source identification.

Choice - 2002-05

Enhanced Methods in Computer Security, Biometric and Artificial Intelligence Systems Jerzy Pejas 2006-07-18

Enhanced Methods in Computer Security, Biometric and Artificial Intelligence Systems contains over 30 contributions from leading European researchers showing the present state and future directions of computer science research. "Methods of Artificial Intelligence and Intelligent Agents" contains 13 contributions analyzing such areas of AI as fuzzy set theory, predicate logic, neural networks, clustering, data mining and others. It also presents applications of AI as possible solutions for problems like firm bankruptcy, soil erosion, flight control and others. "Information Technology Security" covers three important

areas of security engineering in information systems: software security, public key infrastructure and the design of new cryptographic protocols and algorithms. "Biometric Systems" comprises 11 contributions dealing with face picture analysis and recognition systems. This chapter focuses on known methods of biometric problem solution as well as the design of new models.

Information Hiding - Fabien A. P. Petitcolas 2003-01-21

This book constitutes the thoroughly refereed post-proceedings of the 5th International Workshop on Information Hiding, IH 2002, held in Noordwijkerhout, The Netherlands, in October 2002. The 27 revised full papers presented were carefully selected during two rounds of reviewing and revision from 78 submissions. The papers are organized in topical sections on information hiding and networking, anonymity, fundamentals of watermarking, watermarking algorithms, attacks on watermarking algorithms, steganography algorithms, steganalysis, and hiding information in unusual content.

Lossless Information Hiding in Images - Zhe-Ming Lu 2016-11-14

Lossless Information Hiding in Images introduces many state-of-the-art lossless hiding schemes, most of which come from the authors' publications in the past five years. After reading this book, readers will be able to immediately grasp the status, the typical algorithms, and the trend of the field of lossless information hiding. Lossless information hiding is a technique that enables images to be authenticated and then restored to their original forms by removing the watermark and replacing overridden images. This book focuses on the lossless information hiding in our most popular media, images, classifying them in three categories, i.e., spatial domain based, transform domain based, and compressed domain based. Furthermore, the compressed domain based methods are classified into VQ based, BTC based, and JPEG/JPEG2000 based. Focuses specifically on lossless information hiding for images Covers the most common visual medium, images, and the most common compression schemes, JPEG and JPEG 2000 Includes recent state-of-the-art techniques in the field of lossless image watermarking Presents many lossless hiding schemes, most of which come from the authors' publications in the past five years